Measurement

Description

Describes best practices associated with measurement for managing the quality of software systems during development. Several measures that have been proposed to characterize specific security-related characteristics are discussed, and the current extent of the practice of software measurement with specific attention to the use of security-related measures is described.

Overview Articles

Name	Version Creation Time	Abstract
Measures and Measurement for Secure Software Development	11/14/08 3:10:55 PM	This article discusses how measurement can be applied to software development processes and work products to monitor and improve the security characteristics of the software being developed. It is aimed at practitioners—designers, architects, requirements specialists, coders, testers, and managers—who desire guidance as to the best way to approach measurement for secure development. It does not address security measurements of system or network operations.

Most Recently Updated Articles [Ordered by Last Modified Date]

Name	Version Creation Time	Abstract
Measures and Measurement for Secure Software Development	11/14/08 3:10:55 PM	This article discusses how measurement can be applied to software development processes and work products to monitor and improve the security characteristics of the software being developed. It is aimed at practitioners—designers, architects, requirements specialists, coders, testers, and managers—who desire guidance as to the best way to approach measurement for secure development. It does not address security measurements of system or network operations.
Predictive Models for Identifying Software Components Prone to Failure During Security Attacks	10/29/08 3:39:56 PM	Sometimes software security engineers are given a product that they not familiar with

		and are asked to do a security analysis of it in a relatively short time. A knowledge of *where* vulnerabilities are most likely to reside can help prioritize their efforts. In general, software metrics can be used to predict fault- and failure-prone components for prioritizing inspection, testing, and redesign efforts. We believe that the security community can leverage this knowledge to design tools and metrics that can identify vulnerability- and attack-prone components early in the software life cycle. We analyzed a large commercial telecommunications software-based system and found that the presence of security faults correlates strongly with the presence of a more general category of reliability faults. This, of course, is not surprising if one accepts the notion that security faults are in many instances a subset of a reliability fault set. We discuss a model that can be useful for identifying attack-prone components and for prioritizing security efforts early in the software life cycle.
Security-Specific Bibliography	10/1/08 2:25:18 PM	Content area bibliography specific to security.
Software Engineering Bibliography	9/29/08 6:05:17 PM	General content area bibliography.

All Articles [Ordered by Title]

Name	Version Creation Time	Abstract
Measures and Measurement for Secure Software Development	11/14/08 3:10:55 PM	This article discusses how measurement can be applied to software development processes and work products to monitor and improve the security characteristics of the software being developed. It is aimed at practitioners—designers, architects, requirements specialists, coders, testers, and managers—who desire guidance as to the best way to

		approach measurement for secure development. It does not address security measurements of system or network operations.
Predictive Models for Identifying Software Components Prone to Failure During Security Attacks	10/29/08 3:39:56 PM	Sometimes software security engineers are given a product that they not familiar with and are asked to do a security analysis of it in a relatively short time. A knowledge of *where* vulnerabilities are most likely to reside can help prioritize their efforts. In general, software metrics can be used to predict fault- and failure-prone components for prioritizing inspection, testing, and redesign efforts. We believe that the security community can leverage this knowledge to design tools and metrics that can identify vulnerability- and attack-prone components early in the software life cycle. We analyzed a large commercial telecommunications software-based system and found that the presence of security faults correlates strongly with the presence of a more general category of reliability faults. This, of course, is not surprising if one accepts the notion that security faults are in many instances a subset of a reliability fault set. We discuss a model that can be useful for identifying attack-prone components and for prioritizing security efforts early in the software life cycle.
Security-Specific Bibliography	10/1/08 2:25:18 PM	Content area bibliography specific to security.
Software Engineering Bibliography	9/29/08 6:05:17 PM	General content area bibliography.